CSET® Article – Fictional Critical Infrastructure Scenario 02.08.2022

Summertime is vacation time, and Scott and his young family are headed for the coast.

The family SUV is full of laughter and sunshine as Scott and his family of four (plus one on the way) are pointed toward the Atlantic Ocean. The hand shovels and plastic buckets are neatly stowed, and the cooler is packed with sandwiches, ginger ale, and mom's homemade fig newtons.

The morning traffic slows and merges as it approaches the intersection near the Chelsea Street Bridge, a scenic 450-foot vertical lift drawbridge, in northeast Boston. Wedged in among the trucks and commuters, Scott slowly works the family Ford closer and closer to the bridge, and closer and closer to the waters of Chelsea Creek. At last, Scott works into position, and is fully committed to the river crossing.

Scott has crossed the Chelsea Street Bridge hundreds of times and knows the drill. Most days he just cruises past the red-and-white safety drop-gates at the entrance and continues on his way. But Scott is soon to find out today will not be like most days.

Moments after rolling past the giant safety gates and onto the first third of the bridge, the gates drop behind him, the warning bells begin to sound, and the tell-tale whine of the bridge motors signal the center section of the bridge is about to go straight up.

Scott slams on the brakes as the cargo truck ahead stops short. He looks left and out his window and sees the metal junction that marks the boundary between the bridge section and the ground section. Just then, then he hears a deep 'clunk' as the anchoring bolts disengage – signaling the final moment before the Chelsea Street Bridge separates.

An audible gasp from his wife in the passenger seat breaks Scott out of his trance, and he realizes he and his family have just one shot at escaping the unthinkable. Scott is too close to the truck ahead to freely get by on either side. And with the drop-gate behind and time running out, reverse is not an option.

Without hesitation, Scott turns the wheel to the left and guns the accelerator.

A howling screech erupts from the passenger side of the vehicle as the door panels scrape against the loading platform of the cargo truck. As Scott fights for inches, the window in the passenger rear door is bent out of true, bursting both inward and outward to shatter safety glass in all directions. Scott's wife screams out, and his 7-year-old in the backseat is covered with glass, crying "Daddy! Daddy! Daddy!"

Up ahead at the other end of the bridge, Scott watches in horror as a tractor trailer pitches and rolls off the far side of the bridge, falling 80 feet and into Chelsea Creek.

Ten seconds and 20 feet later, the scarred and battered family Ford is up and to the left of the truck – with four feet safely on the bridge as it rises slowly and sanely into the morning sky.

Fictional? Yes. Plausible in the age of aging critical infrastructure system technology. Also yes.

More than plausible, however, the Chelsea Street Bridge actually went up with a pick-up truck in the middle in January 2022.

How is this possible? Well, the answer is more technical than titillating. In short — aging infrastructure control systems are subject to the same effects of aging as the physical infrastructure itself. Systems that

were “state-of-the-art” in the early 2000s can no longer be updated due to the age of the software. It would be like trying to put motor oil in a Tesla – just not compatible technologies.

In addition, these aging systems have proven to be reliable with a great track record, just like Grandpa’s old truck. If it ain’t broke, why fix it? Operators see little reason to make significant upgrades to these systems, especially when there are other critical infrastructure systems that have greater need and require regular attention to function at all.

Scott and his family’s fictional experience on the Chelsea Street Bridge provides a scenario that underscores what may be possible as aging “at risk” critical infrastructure enters the age of cyber vulnerability, both malicious and inadvertent.

Although this scenario is indeed frightening, the Cyber Security Infrastructure Security Agency (CISA) works diligently to thwart such scenarios. CISA provides services and tools to mitigate and reduce the risk of cyber threats to critical infrastructure. CISA funds and guides the development of CSET®, the Cyber Security and Evaluation Tool, which was developed by CISA cybersecurity professionals.

CSET® allows stakeholders to execute cyber assessments to establish a baseline of their cybersecurity posture so they know where they stand. The CSET® tool offers asset owners recommendations on how to bolster an organization’s cyber position and provides recommendations on how to strengthen it. It assists in protecting key national cyber assets and provides users a systematic and repeatable approach for assessing their cyber systems and networks.

CSET® includes both high-level and detailed questions related to all Industrial Control and Industrial Technology systems. The CSET® tool is free to users, and flexible enough to guide a novice on how to establish a basic baseline. It can also be used by expert assessors as they “drill deep” into the granular makeup of an enterprise environment. CSET® is based on industry standards and supports regulation and compliance-based questions, maturity models, and ransomware risk. CSET® is flexible and adaptable enough to support both small establishments and large enterprise organizations. CISA has received positive feedback from users including small organizations who were helped by CSET® when they didn’t know where to start and others who discovered risks they were unaware of and who learned how to effectively mitigate them. CSET® has been downloaded and used by almost 85,000 asset owners and is available on the CISA GitHub website, located at the link provided below.

As overseers of critical infrastructure, asset owners may ask themselves if they have done enough to protect critical assets. If a scenario like Scott’s happened on your watch, what would the repercussions be? What about the legal, financial, moral, and public response? What steps have been taken to reduce the risk and how often do we circle back to re-assess?

If you are an asset owner and are already familiar with CSET®, please know that new updates to CSET® are coming. The current version is 11.0.1, so stay tuned. If you are aware of an asset-owner that is not familiar with CSET®, please share with them the CSET® GitHub link and let them know what CSET® can do for them. Let’s do our part to secure our critical infrastructure so a scenario like Scott’s never plays out during our watch.

https://github.com/cisagov/cset

https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr